UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALICE ORTIZ,

Plaintiff,

v.

PERKINS & CO, et al.,

Defendants.

Case No. 22-cv-03506-KAW

ORDER GRANTING MOTION TO DISMISS

Re: Dkt. No. 15

On June 14, 2022, Plaintiff Alice Ortiz filed the instant case against Defendant Perkins & Co., alleging that Defendant failed to properly secure and safeguard Plaintiff's information -- including her full name, financial account information, and social security number -- on its information network. (Compl. ¶ 1, Dkt. No. 1.) Pending before the Court is Defendant's motion to dismiss. (Def.'s Mot. to Dismiss, Dkt. No. 15.)

Having considered the parties' filings, the relevant legal authorities, and the arguments made at the October 6, 2022 hearing, the Court GRANTS Defendant's motion to dismiss.

I. BACKGROUND

Defendant is an accounting firm who uses a vendor, Netgain, to store data in the cloud. (Compl. ¶ 33; Def.'s Mot. to Dismiss, Exh. A ("Notice").[1] Around May 26, 2022, Defendant sent

[1] Exhibit A is the Notice that Defendant sent to affected individuals, which is available on the California Attorney General's Office. Although the complaint does not attach the Notice to the complaint, the "incorporation by reference" doctrine "permits [a court] to take into account documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the plaintiff's pleading." *Knievel v. ESPN*, 393 F.3d 1068, 1076 (9th Cir. 2005); *see also United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) ("Even if a document is not attached to a complaint, it may be incorporated by reference if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim."). Here, Plaintiff refers specifically to the Notice and its contents for all facts related to the data breach. (Compl. ¶¶ 33, 35.)

a Notice to Plaintiff, stating that between November 8, 2020 and December 3, 2020, an attacker had accessed Netgain's servers storing Defendant's files, some of which were copied and stolen. (Compl. ¶ 33; Notice at 1.) The attacker also encrypted files and demanded a ransom in exchange for returning copies of the stolen files and an access key to the encrypted files. (Notice at 1.) After Netgain paid the ransom, the attacker returned the stolen files and provided a decryption key. (Compl. ¶ 33; Notice at 1.) The Notice noted that Defendant's computer systems were not impacted by the attack. (Notice at 1.) Defendant offered complimentary credit monitoring and identity restoration, and also encouraged recipients to "remain vigilant against incidents of payment card fraud or misuse, to review your account statements, and to monitor your credit reports for suspicious activity." (Notice at 2-3.) As a result of the data breach, Plaintiff alleges that she spent and will continue to spend time dealing with the breach, including verifying the legitimacy of the breach, exploring credit monitoring and identity theft insurance options, monitoring her accounts, and seeking legal counsel. (Compl. ¶ 17.) Plaintiff further alleges that she suffered lost time, annoyance, and anxiety as a result of cyber-criminals accessing her information. (Compl. ¶ 19.)

On June 14, 2022, Plaintiff filed the operative complaint, alleging claims for: (1) negligence, (2) breach of implied contract, (3) breach of the implied covenant of good faith and fair dealing, and (4) unjust enrichment. On August 11, 2022, Defendant filed the instant motion to dismiss. On August 25, 2022, Plaintiff filed her opposition. (Pl.'s Opp'n, Dkt. No. 18.) On September 1, 2022, Defendant filed its reply. (Def.'s Reply, Dkt. No. 21.)

II. LEGAL STANDARD

A. Motion to Dismiss under Rule 12(b)(1)

A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1). A Rule 12(b)(1) motion tests whether a complaint alleges grounds for federal subject matter jurisdiction. A motion to dismiss for lack of subject matter jurisdiction will be granted if the complaint on its face fails to allege facts sufficient to establish subject matter jurisdiction. *See Savage v. Glendale Union High Sch.*, 343 F.3d 1036, 1039 n.2 (9th Cir. 2003). In considering a Rule 12(b)(1) motion, the Court "is not restricted to the

face of the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction." *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988). Once a party has moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the court's jurisdiction. *See Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010).

B. Motion to Dismiss under Rule 12(b)(6)

Under Federal Rule of Civil Procedure 12(b)(6), a party may file a motion to dismiss based on the failure to state a claim upon which relief may be granted. A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the claims asserted in the complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001).

In considering such a motion, a court must "accept as true all of the factual allegations contained in the complaint," *Erickson v. Pardus*, 551 U.S. 89, 94 (2007) (per curiam) (citation omitted), and may dismiss the case or a claim "only where there is no cognizable legal theory" or there is an absence of "sufficient factual matter to state a facially plausible claim to relief." *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 677-78 (2009); *Navarro*, 250 F.3d at 732) (internal quotation marks omitted).

A claim is plausible on its face when a plaintiff "pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citation omitted). In other words, the facts alleged must demonstrate "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

"Threadbare recitals of the elements of a cause of action" and "conclusory statements" are inadequate. *Iqbal*, 556 U.S. at 678; *see also Epstein v. Wash. Energy Co.*, 83 F.3d 1136, 1140 (9th Cir. 1996) ("[C]onclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss for failure to state a claim."). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully . . . When a complaint pleads facts that are merely consistent with a defendant's

liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557) (internal citations omitted).

Generally, if the court grants a motion to dismiss, it should grant leave to amend even if no request to amend is made "unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (citations omitted).

III. DISCUSSION

A. Standing

Article III standing requires the demonstration of three elements: (1) the plaintiff suffered an "injury in fact" that is concrete and particularized and actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Absent this showing, the action must be dismissed. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 109-10 (1998).

Here, Plaintiff asserts the following injuries: (1) the increased risk of future fraud, and (2) lost time from dealing with the data breach. (Pl.'s Opp'n at 5-6.) With respect to the increased risk of future fraud, Defendant argues that per the Supreme Court's recent decision in *TransUnion LLC v. Ramirez*, "the mere risk of future harm, without more, cannot qualify as a concrete harm sufficient to establish standing." (Def.'s Mot. to Dismiss at 6 (citing 141 S. Ct. 2190, 2211).)

In *TransUnion*, the Supreme Court found that there was no standing where the credit reporting company had mislabeled the plaintiffs as potential terrorists in the company's internal credit files, but had never provided those plaintiffs' credit information to any third-party. 141 S. Ct. at 2209. While the plaintiffs argued that the existence of the inaccurate information "in their internal credit files exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm," the Supreme Court found that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm--at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm." *Id.* at 2210-11. Rather, the Supreme Court found persuasive TransUnion's argument that:

> if an individual is exposed to a risk of future harm, time will eventually reveal whether the risk materializes in the form of actual harm. If the risk of future harm materializes and the individual suffers a concrete harm, then the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages. If the risk of future harm does *not* materialize, then the individual cannot establish a concrete harm sufficient for standing[.]

Id. at 2211.

In her opposition, Plaintiff neither acknowledges nor addresses *TransUnion*, instead relying on pre-*TransUnion* cases. (Pl.'s Opp'n at 5.) Specifically, Plaintiff cites *Krottner v. Starbucks Corp.*, in which the Ninth Circuit found standing could be established where "a plaintiff faces a credible threat of harm, and that harm is both real and immediate, not conjectural or hypothetical." 628 F.3d 1139, 1143 (9th Cir. 2010). There, the Ninth Circuit found a credible threat of harm where a laptop containing the unencrypted names, addresses, and social security numbers of 97,000 employees was stolen. *Id.* Plaintiff also cites *In re Zappos.com, Inc.*, which affirmed *Krottner* and found adequate injury in fact because the information stolen in a data breach could be used to commit identity theft. 888 F.3d 1020, 1027-28 (9th Cir. 2018).

Following *TransUnion*, the district courts have split on whether *In re Zappos.com, Inc.* and *Krottner* remain good law. In *I.C. v. Zynga, Inc.*, the district court found that "in light of *TransUnion*'s rejection of risk of harm as a basis of standing for damages claims, the Court questions the viability of *Krottner* and *Zappos*'s holdings finding standing on this very basis." *I.C. v. Zynga, Inc.*, No. 20-cv-01539-YGR, 2022 U.S. Dist. LEXIS 112601, at *32 n.15 (N.D. Cal. Apr. 29, 2022). In contrast, in *Riordan v. Western Digital Corp.*, the district court found that *Krottner* "provides a good point of contrast" to *TransUnion's* concerns regarding speculative allegations of harm. No. 5:21-cv-06074-EJD, 2022 U.S. Dist. LEXIS 101685, at *10 (N.D. Cal. June 7, 2022).

The Court finds that by itself, the risk of increased future harm is not sufficient to establish standing post-*TransUnion*. The Court, however, finds that the time spent dealing with the harm is a cognizable injury where, as here, the information stolen could be used to commit identity theft. *See Clemens v. ExecuPharm Inc.*, No. 21-1506, -- F. 4th --, 2022 U.S. App. LEXIS 24808, at *14 (3d Cir. Sep. 2, 2022) ("Following *TransUnion*'s guidance, we hold that in the data breach

context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he alleges that the exposure to the substantial risk caused additional, currently felt concrete harms. For example, if the plaintiff's knowledge of the substantial risk of identity theft caused him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury."). This is consistent with *TransUnion*, which specifically noted the lack of "present evidence that the class members were independently harmed by their exposure to the risk itself--that is, that they suffered some other injury (such as an emotional injury) from the mere risk that their credit reports would be provided to third-party businesses." 141 S. Ct. at 2211.

In response, Defendant relies on *Clapper v. Amnesty International, USA*, in which the Supreme Court explained that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 568 U.S. 398, 416 (2013). There, however, the plaintiffs took action to avoid government surveillance under § 1881a, but the plaintiffs had "no actual knowledge of the Government's § 1881a targeting practices," such that they could only "speculate and make assumptions about whether their communications with their foreign contacts will be acquired under § 1881a." *Id.* at 411. Moreover, the likelihood of surveillance "relie[d] on a highly attenuated chain of possibilities," requiring that the government target the plaintiffs' foreign contacts, invoke its authority under § 1881a rather than another method of surveillance, have the request approved by the Foreign Intelligence Surveillance Court, and have the plaintiffs' communications included in the communications intercepted by the government. *Id.* at 410. In short, the plaintiffs could not establish standing based on actions taken to avoid harm that was purely speculative.

The harm Plaintiff was trying to avoid here, however, is not speculative. As an initial matter, the stolen information in this case included social security numbers, which courts have recognized as creating a sufficient likelihood of future identity theft. *See Greenstein v. Noblr Reciprocal Exch.*, No. 21-cv-04537-JSW, 2022 U.S. Dist. LEXIS 30228, at *10 (N.D. Cal. Feb. 14, 2022) (finding that the revealing of "highly sensitive personal data, such as social security numbers" will "increase the risk of immediate future harm to the plaintiff"); *Coffey v. OK Foods*

Inc., No. 2:21-CV-02200, 2022 U.S. Dist. LEXIS 42765, at *8 (W.D. Ark. Mar. 10, 2022) ("Here, unlike in *TransUnion* where the possibility TransUnion could disseminate the false reports was speculative, there is no dispute that Plaintiff's name and Social Security number were part of a data breach and accessed by an unknown third party, and Plaintiff has demonstrated a sufficient likelihood this information could cause future identity theft."); *contrast with Zynga, Inc.*, 2022 U.S. Dist. LEXIS 112601, at *29 (finding that associated costs and stress were conjectural because the information stolen -- e-mail addresses, Zynga usernames and passwords, Facebook usernames, phone numbers, and dates of birth -- could not be used to commit identity theft without names and social security numbers). Moreover, in *Remijas v. Neiman Marcus Group, LLC*, the Seventh Circuit found that time and money spent to protect from future identity theft and fraudulent charges were actual injury. 794 F.3d 688, 692-94 (7th Cir. 2015). Distinguishing *Clapper*, the Seventh Circuit found that "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the . . . data breach. Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Id.* at 693. Moreover,

> An affected customer, having been notified by Neiman Marcus that her card is at risk, might think it necessary to subscribe to a service that offers monthly credit monitoring. It is telling in this connection that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information and who had shopped at their stores between January 2013 and January 2014. It is unlikely that it did so because the risk is so ephemeral that it can safely be disregarded.

Id. at 694.

Such is the case here. This is not a situation where, like *Clapper*, the chance of the stolen information being fraudulently used is so "ephemeral" that it is merely speculative. Rather, as Defendant acknowledged before recommending that Plaintiff and other affected parties monitor their accounts, "we still consider any data viewed or stolen by the attacker to be at risk." (Notice at 1, 3.)

In the alternative, Defendant argues that Plaintiff cannot demonstrate standing to pursue injunctive relief because injunctive relief is limited to "*this* data breach." (Def.'s Mot. to Dismiss

at 5.) But injunctive relief is not limited only to preventing harm from a single incident; rather, a plaintiff can seek prospective injunctive relief by "demonstrate[ing] that he has suffered or is threatened with a concrete and particularized legal harm, coupled with a sufficient likelihood that he will **again** be wronged in a similar way." *Bates v. UPS*, 511 F.3d 974, 985 (9th Cir. 2007) (emphasis added). The more fundamental problem that Defendant identifies, however, is that here, it was not Defendant's systems that were compromised, but Netgain's. (Def.'s Mot. to Dismiss at 5.) Plaintiff fails to explain in her opposition how Defendant taking measures such as requiring internal personnel to run automated security monitoring, creating firewalls, conducting regular database scanning and securing checks, or implementing tests of their employees' knowledge of data security would prevent *Netgain* from being breached in the future.

Accordingly, the Court finds that at the pleading stage, Plaintiff can establish standing based on her lost time spent dealing with the data breach for damages purposes, but not injunctive relief. The Court will give Plaintiff leave to amend the complaint to demonstrate injunctive relief is appropriate. In the meantime, the Court considers whether Plaintiff's claims are adequately pled.

B. Negligence

Plaintiff's first claim is for negligence. To plead negligence, Plaintiff must show that Defendant "owed [Plaintiff] a legal duty, that it breached the duty, and that the breach was a proximate or legal cause of [Plaintiff's] injuries." *Merrill v. Navegar, Inc.*, 26 Cal. 4th 465, 477 (2001).

First, Defendant argues that Plaintiff fails to demonstrate actual harm or damages. (Def.'s Mot. to Dismiss at 11.) As previously discussed, the Court finds that there were damages from the time spent dealing with the data breach. Courts have found such lost time to be sufficiently concrete and non-speculative. *See In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 U.S. Dist. LEXIS 80736, at *12 (S.D. Cal. May 7, 2020) ("Increased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by other courts to be specific, concrete, and non-speculative."); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (N.D. Cal. 2019).

Second, Defendant argues that Plaintiff has failed to demonstrate Defendant was the proximate cause of any injury from the data breach because, again, it was not Defendant's computer system that was breached but Netgain's. (Def.'s Mot. to Dismiss at 12.) Plaintiff, in turn, argues that the mere fact that Defendant "collected her information, provided her information to a third party, and sent her the letter informing her of the data breach" makes causation "self-evident." (Pl.'s Opp'n at 8.) The Court disagrees. While it is certainly possible that both Defendant and Netgain may have breached some duty, it is far from a foregone conclusion. Did Defendant knowingly choose a vendor with a history of data breaches? Did Defendant keep information on the cloud server that it should not have? If so, what specific duties did this breach? Plaintiff fails to explain with any specificity, instead pointing to a litany of generic data security practices such as monitoring and restricting access to unsecured information, supervising financial information, enforcing security policies, and implementing policies to detect data breaches. (Compl. ¶ 79.) Plaintiff cannot simply rely on the breach of Defendant's vendor to demonstrate negligence by Defendant; Plaintiff needs to specifically explain the duties that *Defendant* breached, and how that breach caused Plaintiff's harm. The Court finds that Plaintiff fails to adequately allege a negligence claim.

C. Breach of Implied Contract and the Covenant of Good Faith and Fair Dealing

Plaintiff brings a claim for breach of an implied contract, alleging that the parties "entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of" Plaintiff's financial information. (Compl. ¶ 94.) Specifically, Defendant required Plaintiff to provide such information as a condition of receiving services from Defendant. (Compl. ¶ 95.)

Plaintiff's conclusory allegations are insufficient to demonstrate that there was an implied contract; Plaintiff merely alleges that Defendant "assured reasonable security over" Plaintiff's information, but it is unclear where this assurance was located (*e.g.*, in a user agreement, privacy policy, or terms of services) or why this created a contract. (Pl.'s Opp'n at 8.) Indeed, as Defendant points out, based on Plaintiff's allegations it is unclear that the parties engaged in any transaction; Plaintiff does not appear to actually allege that she hired Defendant for any service.

(Def.'s Mot. to Dismiss at 13.) Indeed, at the hearing, Plaintiff's counsel stated that he did not know the nature of the relationship between the parties.

Moreover, several courts have specifically found that consideration is required for an implied contract claim regarding data security. For example, in *Gardiner v. Walmart*, the district court rejected a similar allegation that the plaintiff "did not receive the benefit of his bargain with [the d]efendants, through which he agreed to pay for goods with the understanding that his payment information would be protected by Defendants." No. 20-cv-04618-JSW, 2021 U.S. Dist. LEXIS 75079, at *16 (N.D. Cal. Mar. 5, 2021). In rejecting the claim, the district court explained that the plaintiff did not allege that the defendant represented that his "purchases included a sum understood by the parties to be allocated toward customer data," or "that the cost of the goods he purchased . . . included some amount attributable to data security as required to support his benefit of the bargain theory." *Id.* at *17-18. Likewise, in *In re Linkedin User Privacy Litigation*, the district court found that the complaint failed to allege that the plaintiffs "actually provided consideration for the security services which they claim were not provided." 932 F. Supp. 2d 1089, 1093 (N.D. Cal. 2013). While the plaintiffs had paid for a premium membership, "the bargain is not for a particular level of security, but actually for the advanced networking tools and capabilities to facilitate enhanced usage of LinkedIn's services." *Id.* Thus, the complaint "d[id] not sufficiently demonstrate that included in [the p]laintiffs' bargain for premium membership was the promise of a particular (or greater) level of security that was not part of the free membership." *Id.*; *see also Huynh v. Quora, Inc.*, No. 18-cv-07597-BLF, 2019 U.S. Dist. LEXIS 235733, at *27 (N.D. Cal. Dec. 19, 2019) (finding no breach of contract claim where the plaintiffs "ha[d] not shown that they paid anything for the asserted privacy protections").

Because Plaintiff fails to allege a contract, implied or otherwise, in which Defendant agreed to provide data security, the Court finds that Plaintiff cannot establish a breach of contract claim. Absent a contract, Plaintiff's breach of the covenant of good faith and fair dealing claim also fails. While doubtful, it is possible Plaintiff could point to specific representations from which the Court may find an implied contract. Likewise, to the extent Plaintiff seeks to amend the complaint to argue that Plaintiff was a third-party beneficiary to an implied contract, Plaintiff's

allegations will need to be consistent with existing case law. Accordingly, both these claims are DISMISSED without prejudice.

D. Unjust Enrichment

Finally, Plaintiff brings an unjust enrichment claim. An unjust enrichment claim requires "receipt of a benefit and the unjust retention of the benefit at the expense of another." *Peterson v. Cellco P'ship*, 164 Cal. App. 4th 1583, 1593 (2008) (internal quotation omitted). Importantly, "[t]he mere fact that a person benefits another is not of itself sufficient to require the other to make restitution therefor. There is no equitable reason for invoking restitution when the plaintiff gets the exchange which he expected." *Id.* (internal quotation omitted).

Plaintiff bases her unjust enrichment claim on Defendant's alleged "failure to disclose its lax data security practices at her expense because of her lost time, diminution in value of her PII, etc." (Pl.'s Opp'n at 10.) Plaintiff, however, utterly fails to identify any benefit that Defendant retained. The fact that Plaintiff lost time does not necessarily mean that Defendant gained from it. It is not apparent from the factual pleadings that Defendant gained *anything* from Plaintiff, particularly if Plaintiff did not hire Defendant for any services. Accordingly, the unjust enrichment claim is DISMISSED without prejudice.

IV. CONCLUSION

For the reasons stated above, the Court GRANTS Defendant's motion to dismiss. Plaintiff may file an amended complaint within **21 days** of the date of this order. If no amended complaint or notice of intent not to file an amended complaint is filed by that date, the Court will dismiss the case pursuant to Federal Rule of Civil Procedure 41(b). *See Edwards v. Marin Park, Inc.*, 356 F.3d 1052, 1065 (9th Cir. 2004) ("The failure of the plaintiff eventually to respond to the court's ultimatum--either by amending the complaint or by indicating to the court that it will not do so--is properly met with the sanction of a Rule 41(b) dismissal.").

IT IS SO ORDERED.

Dated: November 2, 2022

Kandis Westmore

KANDIS A. WESTMORE
United States Magistrate Judge